METHOD OF MAINTAINING INTEGRITY OF AN INSTRUCTION OR DATA SET

ABSTRACT

In combination with a computer system having a special modifiable memory, such as Flash ROM or a system partition of a hard disk drive, in which is loaded an original code set, a method for maintaining the integrity of the contents of that modifiable memory when the system attempts to overwrite the contents with a different code set. The developer of a code set (e.g., a BIOS) that is generally stored in a modifiable memory selects a one-way algorithm, which is maintained as a company secret. Whenever a new version of the code is made available, whether as a downloadable Internet file or on a removable medium, the loadable code is always accompanied by a security key which was generated by having the one-way function operate on the new code set. In order to prevent unauthorized modifications to code stored in a modifiable memory, a computer system is equipped with a custom memory controller having an embedded, hard-wired copy of the secret one-way function. The system applies the embedded one-way function to the new code version and calculates a local. The local key is compared with the security key. If two keys match, the memory controller permits the new code version to be loaded into the modifiable memory.